University of Maryland
HIPAA General Operating Policy
Regarding the Privacy of Health Information
("HIPAA Privacy Policy")
Adopted April 14, 2003

I. General

The University of Maryland includes units, such as the University Health Center, that provide health care to individuals, including students, staff, visitors, and others. Other University units may have access to information related to this health care because of their activities in support of health care provider units. It is the policy of the University that the confidentiality of health care related information and the privacy of individuals should be protected to the maximum extent feasible, in accordance and consistent with: the Federal Health Insurance Portability and Accessibility Act of 1996 (HIPAA)[1]; the Family Educational Rights and Privacy Act (FERPA);[2] applicable Maryland State Law;[3] the ethical standards of the health professions; and the general responsibility of the University to support the privacy rights and concerns of its members.

This document specifically refers to University policy concerning its privacy obligations under HIPAA. It is intended to provide general operating guidelines for HIPAA compliance. Except as permitted by HIPAA to comply with certain Maryland state reporting requirements or other Maryland laws that provide greater individual privacy rights or protections regarding health information, this Policy will be implemented in accordance with the HIPAA Privacy Rule,[4]

II. Applicability

The University has declared its status as a "Hybrid Entity" under HIPAA and has designated those units that comprise its HIPAA covered "Health Care Component."[5] The University's designated Health Care Component includes certain units that provide health care and thereby develop health care information about individuals, and other units that have access to this information for the purpose of assisting the health care provider units in performing various functions, including treatment, payment, and other health care related operations.

This policy applies only to those units that are designated as part of the covered Health Care Component ("covered units"). Although other units may voluntarily choose to

---

[1] 42 U.S.C. §1320d, 45 CFR Parts 160, 162, and 164.

[2] 20 U.S.C. §1232g

[3] Md. Code Ann., Health General Article, §§4-301 *et seq.*

[4] 45 CFR Parts 160,(see http://www.access.gpo.gov/nara/cfr/waisidx_02/45cfr160_02.html), 162 (see http://www.access.gpo.gov/nara/cfr/waisidx_02/45cfr162_02.html), and 164 (see http://www.access.gpo.gov/nara/cfr/waisidx_02/45cfr164_02.html).

[5] *See* UM Policy on HIPAA Compliance posted *at* http://hipaa.umd.edu .

comply with this policy, in whole or in part, such voluntary compliance shall not affect a unit's status as a non-covered component. For the purpose of this policy, disclosures to University units outside the designated Health Care Component are to be treated in the same manner as disclosures to outside entities.

III. Definitions

The definition of key terms in this policy are as set forth in the applicable HIPAA privacy regulations. *See* 45 CFR 160.103 and 45 CFR 164.501.

IV. Protected Health Information (PHI)

This policy applies to all faculty, staff, students, volunteers and any other personnel in the designated Health Care Component who have access to "Protected Health Information" (PHI). As defined by HIPAA, PHI includes individually identifiable health information[6] in any form--written, oral or electronic.

PHI does not include employment records held by the University in its role as an employer; nor does it apply to student records or information covered by FERPA or student treatment records expressly excluded by FERPA. Such employee and student records and information are subject to the requirements of FERPA and/or State law regarding student, personnel and/or medical records, as applicable, and are protected under provisions of those laws and applicable University policy.[7]

V. Confidentiality and Minimum Necessary Standards

A. Confidentiality

PHI is to be treated confidentially and in such a manner as reasonably to protect it from being intentionally or unintentionally seen, overheard or intercepted by those without a need or right to know. Each covered unit is responsible for implementing procedures that reasonably protect the confidentiality of oral, written and electronic communications and other health information in any form.

B. Minimum Necessary [45 CFR 164.502(b); 164.514(d)]

PHI should be accessed, used and disclosed only by authorized personnel. Except for disclosures or requests related to treatment or pursuant to individual authorization or as otherwise permitted or required by law, a covered unit must make reasonable efforts to limit the PHI it uses, discloses or requests to the the minimum amount reasonably necessary to accomplish the intended purpose.

---

[6]Individually identifiable health Information is any information (including demographic information), whether oral or recorded in any form, that: is created or received by the Health Care Component; relates to an individual's past, present, or future physical or mental health or condition, or to the provision of or payment for health care, past present or future; and either identifies the individual or could be used to identify the individual.

[7]*See, e.g.*, UM Policy and Procedures on the Disclosure of Student Education Records (III-6.30(A))

Each covered unit is responsible for identifying the persons or classes of persons who need access to PHI to carry out their job duties and for identifying the type(s) of health information for which access is needed, as well as any appropriate conditions on such access. Each covered unit is responsible for implementing procedures that limit the PHI it uses, discloses or requests to the minimum amount necessary to accomplish the intended purpose.

VI. Uses and Disclosures of PHI with Authorization [45 CFR 164.508]

PHI may be used or disclosed pursuant to a valid written Authorization signed by the individual or his/her personal representative.[8] An Authorization must contain the elements required by HIPAA[9] and/or applicable Maryland law. An individual may revoke an authorization in writing except to the extent action has been taken in reliance on it. The Health Care Component may not require an individual to sign an Authorization as a condition of providing treatment, payment or other benefits except in certain circumstances for research related treatment and for health care which by its nature requires disclosure of PHI to a third party.

VII. Uses and Disclosures of PHI without Authorization

A. Treatment, Payment and Health Care Operations [45 CFR 164.506]

PHI may be used or disclosed without Authorization[10] by the Health Care Component for treatment, payment and health care operations purposes.

B. Business Associates [45 CFR 164.502 and 164.504]

A covered unit may disclose PHI to "Business Associates,"[11] who provide services that utilize health information (e.g., software firms, telecommunications providers, computer support personnel, lawyers, accountants, consultants, accrediting agencies). Except for disclosures to a health care provider regarding treatment of an individual, PHI may only be shared with a Business Associate pursuant to a Business Associate Agreement approved by the University's Privacy Officer.

Business Associate Agreements must be in writing and signed by the appropriate parties

---

[8]Except as required or permitted by law, a covered unit must treat a legally authorized personal representative as the individual for purposes of this policy.

[9]*See* 45 CFR 164.508(c).

[10]The use of psychotherapy notes requires an Authorization, except for use by the originator for treatment and for certain operations activities. *See* 45 CFR 164.508(a)(2).

[11]A Business Associate is a person or entity outside the Health Care Component that performs or assists the Health Care Component in preforming activities that involve the use or disclosure of individually identifiable health information. Such activities include claims processing or administration, data analysis, accounting, billing, utilization or quality review, legal or financial services, accreditation, etc. *See* 45 CFR 160.103.

prior to disclosure of any PHI. Business Associate Agreements must provide satisfactory assurances that the Business Associate will appropriately safeguard any PHI it receives or creates in accordance with HIPAA requirements. If a covered unit learns that a Business Associate has violated a material term or obligation relating to HIPAA compliance, the unit shall notify the University's Privacy Officer.

C. Permission or Opportunity to Object [45 CFR 164.510]

A covered unit may use or disclose PHI in certain circumstances, if the individual is informed in advance of the use or disclosure and has been given the opportunity to object. The circumstances include: 1)providing directory type information (*e.g.*, name, location in the facility and general condition) to family, friends, clergy and others who ask for the patient by name; 2)providing relevant information to family, friends and others involved in a patient's care or payment for healthcare ; 3) providing information when the patient is present and does not object; and 4) providing information to appropriate entities for disaster relief purposes .

For these purposes, notice may be provided, and permission may obtained, orally. Notice and opportunity to object is not required in emergency situations, or when the individual is incapacitated or is not present. In such circumstances, a health care provider unit may disclose such relevant information as it determines to be in the best interest of the patient, so long as disclosure is not inconsistent with a previously expressed preference or restriction. A unit may similarly use professional judgment and experience to allow a person to act on behalf of an individual to pick up prescriptions, medical supplies, x-rays or similar types of PHI.

D. Disclosures Required by Law and Similar Purposes Not Requiring Authorization or Opportunity to Object [45 CFR 164.512]

A covered unit may use or disclose PHI without Authorization and without providing an opportunity for an individual to agree or object if the use or disclosure is: 1)required by law; 2)permitted by law for public health activities; 3)related to victims of abuse, neglect or domestic violence; 4)for government health oversight activities; 5) for judicial and administrative proceedings; 6)for certain law enforcement purposes; 7)about decedents, to coroners, medical examiners and funeral directors; 8)for cadaveric organ, eye or tissue donation purposes; 9)for certain research purposes, as set forth in item E. below; 10)to avert a serious threat to the health or safety of a person or the public; 11) for specialized government functions such as military and veterans activities, national security and intelligence activities, correctional institutions and other law enforcement custodial situations, etc.; and 12)for workers' compensation compliance.

All uses or disclosures for these purposes shall conform to any conditions or requirements imposed by HIPAA and/or Maryland law, as applicable.

E. Research [45 CFR 164.501, 164.508, 164.512(i), 164.614(e), 164.528, 164.532]

The Health Care Component may use or disclose PHI without individual authorization for research purposes in the following circumstances: 1)upon obtaining documentation

of Institutional Review Board (IRB) approval of a waiver or alteration of authorization requirements;[12] 2)for reviews preparatory to research (*e.g.*, to design or assess the feasibility of conducting a study) if the researcher provides appropriate assurances;[13] 3)for research on decedents' PHI, with appropriate assurances from the researcher;[14] and 4)for disclosure of de-identified PHI or limited data sets, as set forth in item VII. F., below. In addition, the researcher must sign an acknowledgment of the duty under Maryland law not to re-disclose the information.

Additional information regarding HIPAA covered research may be found on the University's IRB website at http://

F. Miscellaneous Uses and Disclosures [45 CFR 164.514, 164.501, 164.502, 164.508(3)]

De-Identified PHI. The Health Care Component may use or disclose PHI that has been "de-identified" by removing all information that could be used to identify an individual. PHI may be considered to de-identified if all potential identifiers listed in HIPAA[15] are removed or a suitable expert determines that the risk is very small that the information, alone or in combination with other available information, could be used to identify an individual.

Limited Data Sets. The Health Care Component may use or disclose PHI that is part of a "limited data set" pursuant to a data use agreement. A limited data set requires the removal of fewer identifiers than de-identified information. However, all direct identifiers (*e.g.*, names, street addresses, telephone and other identification numbers) must still be removed, as required by HIPAA ;[16] only indirect potential identifiers (*e.g.*, cities, states, zip codes, and certain dates) may be included in a limited data set. A data use agreement provide satisfactory assurance that the recipient will use or disclose the PHI for limited purposes and must be approved by the University's Privacy Officer.

Marketing and Fundraising. The Health Care Component may use or disclose PHI for marketing purposes only with an individual's Authorization; however, communications

---

[12]For a description of the IRB documentation required, see IRB website *at* _____ and 45 CFR 164.512(i)(1)(i).

[13]The researcher must represent (orally or in writing) that: the use or disclosure is solely to prepare a research protocol or for a similar preparatory purpose; PHI will not be removed from the covered entity; and access to the PHI is necessary for the research purpose. [45 CFR 164.512(i)(1)(ii)].

[14]The researcher must represent (orally or in writing) that the use or disclosure is solely for research on the PHI of decedents and the PHI sought is necessary for the research. The covered unit may also request documentation of the death of the individual(s). [45 CFR 164.512(i)(1)(iii)].

[15]Listed identifiers include names; telephone & fax numbers; all geographic designators; email addresses; all elements of dates; social security numbers; all ages over 89; urls & ip numbers; medical records numbers; full face photographic images; health plan beneficiary numbers; biometric identifiers; account numbers; certificate/license numbers; vehicle identifiers & serial numbers; license numbers; and any other unique identifying number, characteristic or code. *See* 45 CFR 164.514(b)(2).

[16]*See* 45 CFR 164.514(e)(1).

about goods and services for treatment or that are otherwise essential for quality health care are not generally considered marketing. Face to face communications between a covered unit and an individual are also generally permitted without authorization.

The Health Care Component may use[17] certain PHI (individual demographic information and dates of health care) without Authorization for its own fund raising purposes, if appropriate notice is provided in its Notice of Privacy Practices (*see* item VIII., below). Any fund raising materials sent to an individual must include an explanation of how to opt out of future fund raising communications, and reasonable efforts must be undertaken to ensure that individuals who opt out do not receive future communications.

VIII. Notice of Privacy Practices [45 CFR 164.520]

A covered unit that provides health care must provide individuals with adequate notice of how it handles PHI (Notice of Privacy Practices). The Notice of Privacy Practices must describe, in plain language: 1)how the unit may use and disclose PHI; 2)the individual's rights with respect to PHI; 3)the University's duties with respect to PHI; and 4)who to contact for further information regarding privacy practices. The Notice must be provided in the form and manner required by HIPAA and must comply with this policy.

The Notice of Privacy Practices must be prominently posted in the health care facility and on the University's website. A copy must be made available to any person who asks for it.

A covered unit that provides health care must provide a copy of the Notice to an individual prior to initial treatment or other delivery of services unless such advance notice is not feasible due to an emergency situation. The health care provider must also make a good faith effort to obtain written acknowledgment of receipt of the Notice from the patient. If such acknowledgment can not be obtained, the unit should document its efforts to obtain it and the reasons why it could not be obtained. Except where patient care might be compromised, a health care provider may condition providing services upon obtaining an acknowledgment of receipt of the Notice from a patient.

Except in emergency or other situations in which patient care might be compromised, PHI should not knowingly be used or disclosed in a way that is inconsistent with a Notice of Privacy Practices.

All Notice(s) of Privacy Practices, and all subsequent changes in such notices, must by approved by the University's Privacy Officer prior to use. The University reserves the right to revise a Notice of Privacy Practices, as deemed necessary or appropriate A Notice must be revised whenever there is a material change in a unit's privacy practices. . Except when required by law, a material change may not be implemented prior to the effective date of the revised Notice that reflects the change.

[17]PHI may also be disclosed to a Business Associate or Affiliated University Foundation for similar fund raising purposes.

IX. Individuals' Rights Regarding PHI

A. Restrictions on Uses and Disclosures [45 CFR 164.522(a)]

The Health Care Component must permit an individual to request restrictions on the use or disclosure of his or her PHI for treatment, payment or health care operations or to family, friends or others involved in his or her health care. The Health Care Component need not agree to a restriction. If the Health Care Component agrees to a restriction, PHI should not be used or disclosed in a way that is not consistent with any restrictions requested by the patient and agreed to by the University, except as needed to provide emergency treatment or as required by law.

A restriction may be terminated upon request or agreement of the individual. A restriction may also be terminated if the covered unit informs the individual that it is terminating its agreement to a restriction; however, such termination is effective only as to PHI that is created or received after notice of the termination is given to the individual.

All restrictions that are agreed to must be appropriately documented. All terminations of restrictions must be appropriately documented.

B. Confidential Communications [45 CFR 164.522(b)]

An individual may request, in writing, that the Health Care Component communicate with him or her at a particular place (*e.g.*, home vs. work) or in a particular manner (*e.g.*, e-mail vs. writing). The Health Care Component may not require an individual to provide an explanation for a request. A request for confidential communications must be accommodated, if it is reasonable. A reasonable accommodation may be conditioned upon the individual providing an alternative address or means of conduct and, if appropriate, information on how payment will be handled.

C. Access, Amendment and Accounting of Disclosures [45 CFR 164.524, 164.526 and 164.528; Md. Code Ann., Health General Article §4-304]

In accordance with HIPAA and applicable State law, it is the policy of the University that individuals be afforded the following rights with respect to their PHI maintained by the Health Care Component: 1)to inspect and obtain copies; 2)to request amendment; and 3) to receive an accounting of disclosures. The University's policies regarding implementation of these rights are separately set forth in the University's HIPAA General Operating Policy–Access, Amendment and Accounting of Disclosures.